

Atty. Docket No.: LYRN006US0
Customer ID No. 58,293

REMARKS:

The Examiner's indication of allowability with respect to claim 16 is gratefully acknowledged.

The Examiner's remarks concerning the claim of priority in the present application under 35 U.S.C. § 120 have been noted. The specification has been amended with this response to specify the relationship of the non-provisional applications cited therein, and to update the status of those applications. It is thus respectfully submitted that the Examiner's request has been complied with.

Reconsideration of the Examiner's rejection of claims 18-23 under 35 U.S.C. § 101 as being directed to non-statutory subject matter is respectfully requested.

Claim 18, from which the remaining rejected claims depend, was amended in the last response to specify that the recited method is a method for encrypting/decrypting data. In the present Office Action, the Examiner argues that the added language does not render the claim statutory, because "it is a field of use limitation because it is only recited in the preamble, and the body of the claim does [not] recite anything that links to 'encrypting/decrypting'".

Accordingly, claim 18 has been further amended with this response to recite claim elements within the body of the claim that link to the recited method of encrypting/decrypting data. It is thus respectfully submitted that the Examiner's rejection has been overcome. In particular, as noted in M.P.E.P. § 2106(IV)(B)(2)(b), a claimed process is statutory if it is "limited to a practical application of the abstract idea or mathematical algorithm in the technological arts." Since encryption/decryption of data is a practical application of the mathematical algorithm described in claim 18, it is respectfully submitted that the presently claimed subject matter is statutory.

Reconsideration of the Examiner's rejection of claims 1, 17 and 24 under 35 U.S.C. § 102(b) as being anticipated by U.S. 4,893,268 (Denman, Jr. et al.) is respectfully requested.

Atty. Docket No.: LYRN006US0
Customer ID No. 58,293

In order for a cited reference to anticipate a claimed invention, the reference must disclose each and every element of the claimed invention. Claim 1 (from which claims 17 and 24 depend) has been amended with this response to incorporate the element of the chaining controller being adapted to instruct the first and second chaining subsets to operate as first and second distinct computational chains when the apparatus is required to perform exponentiations of first and second sizes, respectively. Since Denman, Jr. et al. does not teach or disclose these features of the presently claimed invention, it is respectfully submitted that the Examiner's rejection has been overcome.

Reconsideration of the Examiner's rejection of claims 1-9, 11, 12, 14, 15 and 17 under 35 U.S.C. § 102(e) as being anticipated by U.S. 6,282,290 (Powell et al.) is respectfully requested.

In order to anticipate a claimed invention, a cited reference must teach each and every element of the claimed invention. In the present case, Powell et al. does not anticipate claim 1 (or claims 2-9, 11, 12, 14, 16 or 17, which are dependent on claim 1) because Powell et al. does not teach, inter alia, a "chaining controller" (described on Page 24, Lines 26-27 as "a controller that associates stations as a computational chain").

One of the principle benefits obtained by the apparatus described in the present application is flexible chaining, which is implemented by the chaining controller. The concept of flexible chaining is described at page 7, lines 3-22 of the present application. As described therein, flexible chaining provides for a more efficient use of computational resources by allowing those resources to be associated into computational chains, depending on the size of the exponentiation to be formed.

Thus, for example, in the embodiment of the computational device illustrated in FIG. 2, the device 10 contains four stations 18, and each station contains two session control devices 24 which can process RSA exponentiations concurrently. The stations operate independently when the computational device is required to process 1K exponentiations. However, the stations are chained together as indicated by chains 20 when the computational device is required to process 2K exponentiations, and are chained together as indicated by chains 22 when the computational device is required to process 4K exponentiations.

Atty. Docket No.: LYRN006US0
Customer ID No. 58,293

As noted at Page 7, Lines 19-22 of the present application, such flexible chaining avoids the waste of excess capacity encountered by computational devices configured with only large-bit exponentiators, and also avoids wasted overhead due to iterating small-bit exponentiators to handle large-bit numbers as faced by non-chaining solutions that have only small-bit exponentiators.

Turning now to the solution presented by Powell et al., it is clear that this solution is not a flexible chain implementation of exponentiation, and it is also clear that the device of Powell et al. lacks a chaining controller. In particular, the computational device described in Powell et al. functions in the same manner regardless of the size of the exponentiation to be performed. Thus, as explained at Col. 4, Lines 45-54 of the reference, in the device described therein, the modular exponentiation is split into components which are processed separately by two separate processing units 24a and 24b. This is analogous to the splitting performed by the cleave/merge engine 42 within the stations 18 depicted in FIG. 2 of the present application. However, Powell et al. neither teaches nor suggests a flexible chaining algorithm of the type disclosed in the present application whereby computational resources may be allocated based on the bit size of the modulus, base and exponent (variables n , b and e in the parlance of Powell et al.), nor does Powell et al. teach a controller that implements such an algorithm.

Indeed, it is clear that Powell et al. does not even teach the concept of chaining. This concept may be appreciated from the definition of a "chaining controller" set forth at Page 24, Lines 26-27 of the present application as "a controller that associates stations as a computational chain". From this definition, it is clear that "chaining" refers to the association of stations into a computational chain.

Reconsideration of the Examiner's rejection of claims 1-3, 5-10, 12, 13 and 17 under 35 U.S.C. § 102(e) as being anticipated by WO 01/29652 (Fairclough et al.) is respectfully requested.

In the previous Office Action, the Examiner rejected the present claims under 35 U.S.C. § 102(e) as being anticipated by U.S. 6,963,979 (Fairclough et al.), which is the national stage filing of the present reference. In their response to that Office Action, Applicants noted that the

Atty. Docket No.: LYRN006US0
Customer ID No. 58,293

filing date of the '979 patent is April 11, 2002, while the filing date of the present application is February 16, 2002. Since the filing date of the '979 patent postdates the filing date of the present application, Applicants noted that the '979 patent does not qualify as prior art under 35 U.S.C. § 102(e), and that the Examiner's rejection therefore lacked statutory basis.

In the present Office Action, the Examiner now seeks to make the same rejection based on the PCT application from which the '979 patent claims priority. However, Applicants respectfully note that this substitution does not overcome the issue that prevented the '979 patent from being prior art under 35 U.S.C. § 102(e). As explained in M.P.E.P. § 2136, the prior art date of a reference under 35 U.S.C. 102(e) is the international filing date *only if the international filing date was on or after November 29, 2000*. If, as is the present case, the PCT application was filed prior to November 29, 2000, the reference is subject to the former (pre-AIPA) version of 35 U.S.C. § 102(e) as set forth below:

A person shall be entitled to a patent unless-

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Since the requirements of 35 U.S.C. § 371(c) in the Fairclough et al. PCT application were not met until April 11, 2002 (i.e., the effective filing date of the '979 patent), the filing date of Fairclough et al. postdates the filing date of the present application. Therefore, even taking into account the filing date of the PCT priority document, Fairclough et al. does not qualify as prior art under 35 U.S.C. § 102(e). Hence, the Examiner's rejection is improper and lacks statutory basis.

With respect to the new claims added with this response, support for these claims may be found, for example, in the claims as originally filed, in FIG. 2, and at Page 7, lines 3-22 of the specification.

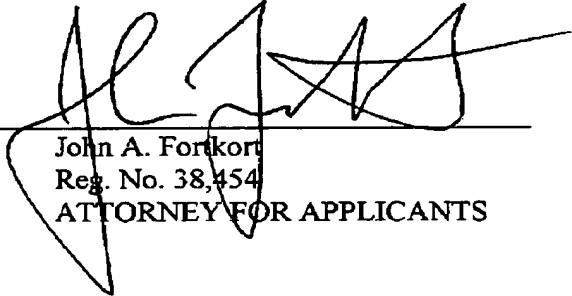
Atty. Docket No.: LYRN006US0
Customer ID No. 58,293

Should the Examiner have any questions or desire clarification of any sort, the Examiner is invited to telephone the undersigned at the number listed below. Please reference Attorney Docket No. LYRN006US0.

A Fee Transmittal is attached hereto authorizing the Commissioner to deduct the extra claim fees from Deposit Account No. 50-3694 of Fortkort & Houston P.C. It is believed no further fee is due with this transmission, however, should a further fee be due or a credit authorized, the Commissioner is authorized to deduct such fee or credit such overpayment to Deposit Account No. 50-3694 of Fortkort & Houston P.C.

Respectfully submitted,
FORTKORT & HOUSTON P.C.

Date: 07 September 2006

By: 
John A. Fortkort
Reg. No. 38,454
ATTORNEY FOR APPLICANTS

9442 N. Capital of Texas Hwy.
Arboretum Plaza One
Suite 500
Austin, Texas 78759
Tel: (512) 343-4525
Fax: (512) 343-4530
jfortkort@foholaw.com